




UNITED STATES DEPARTMENT OF COMMERCE
Chief Information Officer
Washington, D.C. 20230

JUN 30 2005

MEMORANDUM FOR: Heads of Operating Units
Chief Information Officers

FROM: Thomas N. Pyke, Jr. 

SUBJECT: DOC IT Security Program Policy and Minimum
Implementation Standards, Revised

I am pleased to announce the issuance of a revised, comprehensive Commerce IT Security Policy. The Policy is titled *Department of Commerce IT Security Program Policy and Minimum Implementation Standards*, and is available online at <http://www.osec.doc.gov/cio/oipr/ITSEC/DOC-IT-Security-Program-Policy.htm>. This revision incorporates all the NIST guidance issued since the initial Policy was issued on January 23, 2003, and it supersedes the revision of the Policy issued on July 28, 2004. This Policy also incorporates several IT security policy memoranda and other related documents, so it provides in one place all current Commerce IT security guidance. Please bring this new Policy to the attention of all your staff who have significant IT security responsibilities.

This Policy represents the foundation of comprehensive rules and practices that regulate access to and protection of all Commerce IT systems and the information processed, stored, and transmitted by them. The Commerce IT Security program management structure described in the Policy establishes the required framework of security controls that ensure compliance with the Federal Information Security Management Act of 2002. The Policy applies to all Commerce operating units and personnel (federal employees and contractors), guest researchers, collaborators, and others requiring access to the hardware and software components that constitute Commerce IT systems. It applies to all Commerce IT systems used to carry out the Department's mission, both non-national security and national security systems. For example, it applies to desktop PC workstations, laptop computers and other portable devices, servers, network devices, office automation equipment (such as copiers and fax machines with communication capabilities), whether or not they are Commerce-owned or leased or contractor-owned and operated on behalf of the Department.

DOC operating units may issue supplemental implementation procedures to describe specific practices for implementing this Policy within each operating unit. This Revised Policy is effective 30 days from the date of this memo. Section 1.9 of the Policy contains specific dates by which compliance with specific parts of the Policy is required.

If you have any questions regarding this Policy, please contact the Department's IT Security Program Manager, Nancy DeFrancesco, at (202-482-3490), or me at (202) 482-4797.